

STATE OF VERMONT
Banking Division

Department of Banking, Insurance, Securities & Health Care Administration

Banking Division Consumer Advisory:

**SCAM WARNING:**
Unsolicited Phone Calls Posing as Credit Unions

The following is an alert from the Vermont Department of Public Safety that we are rebroadcasting on the Banking Division website. We note that other credit union names besides those listed below may be used in the scam. If you have followed the automated caller's prompts and given out your pin number, contact your financial institution immediately to terminate your card.

STATE OF VERMONT
DEPARTMENT OF PUBLIC SAFETY
VERMONT STATE POLICE
PRESS ADVISORY

For Release: March 13, 2009
Contact: Lieutenant Mark Lauer

(802) 872-6111

Law Enforcement Agencies across the state of Vermont are receiving complaints from citizens indicating that they are receiving unsolicited phone calls regarding credit cards accounts. The automated messages may indicate they are calling from one of the three institutions:

NCUA (National Credit Union Administration)

Central Vermont Medical Center Credit Union

Members Advantage Credit Union.

All of the calls were pre-recorded messages that said that the user's credit card had been frozen because of a possible fraud attempt on the card. The automated message prompted the recipient to push #1 and follow the directions to reactivate the card. The caller was then instructed that they would be asked 3 security questions.

The recipient was then prompted to enter their credit card number, PIN Number and the Security Code printed on the Card.

The Vermont State Police would like to remind you to follow these safety precautions when dealing with your personal information:

Whether you've misplaced a credit card or had a purse or wallet stolen, the loss of personal identification and financial information can be a major concern. The number of people who have their identities stolen every year is growing, and countless more suffer credit card loss or theft. Knowing the right precautions to take can help safeguard your financial freedom and prevent devastating losses to your cash reserves and credit rating.

Try these suggestions to deter financial and personal ID thieves:

- * Make a list of all your credit cards, accounts and memberships. Write down the company name, account number, address and toll-free phone number, and then store this list in a safe, secret place (not on your person). Be sure to keep the list updated, adding any new cards or accounts you obtain to this list.
- * Handle Personal Identification Numbers (PINs) carefully. Never carry a written PIN with you. Create unique PINs (don't use your birth date, any part of your name or maiden name, Social Security Number or anything else that could be easily identified by thieves), and memorize them.
- * Sign the back of any new credit card in permanent ink or write "Ask for Identification" to prevent unauthorized persons from using your card.
- * Carry only those cards that are necessary for the trip you're making. Try to carry these cards separately from your wallet or purse if you can, in a zippered compartment, secure pocket or small pouch, for example.
- * Reduce high limit balances on credit cards to an amount that you need.
- * Do not use your mother's maiden name as a form of security information.
- * Never give a clerk or cashier any personal information when using your credit cards. By law, you are not required to give out this information. Also, if you are paying by check and the cashier requires a credit card as identification, don't allow the cashier to write down your credit card number on your check.
- * Ask your department of motor vehicles to issue you a random license number rather than using your Social Security Number.
- * Watch your credit card carefully during each transaction. Be sure other shoppers cannot read the card. Don't allow the cashier to take your card away from the register and get your card back as quickly as possible.
- * Never sign a blank receipt. Draw a line through any blank spaces. Be sure the total box is filled in.
- * Shield your card and the ATM monitor whenever you use a cash machine. Also, shield your card and the telephone whenever you use a calling card.
- * Never lend your card to anyone.
- * Cancel all unnecessary cards that you don't plan to use. Call the issuer to request that the card be cancelled, and then cut up the card in several pieces. Have the issuer verify your request in writing.
- * Use a crosscut shredder to destroy all credit card and ATM receipts, bills, check carbons and account statements after you have verified their accuracy. Also, remember to destroy unsolicited pre-approved credit card applications that arrive in the mail.
- * Check your monthly billing and account statements promptly when they arrive. Reconcile these accounts and resolve any disputes with card issuers, financial institutions and vendors as necessary. Remember that you have the right to withhold payment for any disputed amount without incurring penalty fees until the

card issuer can investigate the matter and render a decision.

* Check your credit reports at least once a year. Request a credit report from the three main credit reporting agencies (typical cost is \$8 a report):

Equifax: (800) 685-1111

Experian: (888) 397-3742

TransUnion: (800) 888-4213

* Unless the company or vendor is a familiar, reputable one you can trust, never give out any account numbers over the phone. This is especially important if someone else made the call. If you feel the call is legitimate, ask the caller for a number where you can call them back, or ask that they mail you more information. If you're not sure about the company, check with your local Better Business Bureau.

* Have your name removed from marketing and junk-mail lists. This can cut down on the number of unsolicited credit card applications (which can be easily stolen) you receive via mail. Call (888) 5-OPT-OUT for details.

* Check to see if your homeowner's insurance policy covers liability for credit card theft. If it doesn't, consider upgrading your policy to provide this coverage.

http://www.dps.state.vt.us/vtsp/id_theft.htm

If you feel you have been the victim of identity theft, contact your local police agency to file a report.

[Return to Banking Division Advisories](#)

.